March 31, 2000

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th and C Streets, N.W.
Washington, D.C. 20551

Mr. Robert E. Fledman
Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, D.C. 20429

Manager
Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552

Communications Division
Office of the Comptroller of the Currency
250 E Street, S.W.
Washington, D.C. 20219

Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Ms. Becky Baker
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428

Mr. Jonathan G. Katz
Secretary
Securities and Exchange Commission
450 5th Street, N.W.
Washington, DC 20549-0609

COMMENTS ON PROPOSED RULES REGARDING PRIVACY OF CONSUMER FINANCIAL INFORMATION

To Whom it May Concern:

We are writing to comment on your proposed rules on standards for protecting the privacy of customers of financial institutions and other persons within the jurisdiction of your respective agencies, which is designed to implement the financial privacy provisions of Subtitle A of Title V of the Gramm-Leach-Bliley Act ("GLBA" or "the Act") (Pub. L. No. 106-102, codified at U.S.C. 6801 et seq.). We commend you for moving forward swiftly with this effort and for the thorough and thoughtful discussion contained in the proposed rule. We believe that the proposed rule is a useful step towards addressing the pressing need for greater financial privacy protections. At the same time, however, we feel that the proposed rule fails to establish adequate privacy protections for consumers. While we believe that modifications to the proposed rule could address some of these failures, we also believe the most serious problems are largely the result of shortcomings in GLBA, which we will describe more fully below. Because there are only minor differences in the rules proposed by each of your agencies, we are taking the liberty of filing identical comments on the proposed rules with each agency.

Overall, we believe that the proposed rules, taken as a whole, fail to provide sufficient protections for the privacy of nonpublic personal information. The rules establish requirements for financial institutions to provide consumers with clear and conspicuous notice regarding the institution's privacy policies and practices. They describe the conditions under which a financial institution may disclose such nonpublic personal information to nonaffiliated third parties. They provide methods for a consumer to "opt out" of the disclosure of nonpublic personal information to certain third parties. They require financial institutions to adopt policies and procedures reasonably designed to: a) insure the confidentiality of customer records and information; b) protect against any anticipated threats or hazards to the security of customer records and information; and c) protect against unauthorized access or use of customer records or information that could result in substantial harm or inconvenience to any consumer.

Despite these positive features, significant gaps in financial privacy protections remain which are not addressed by the proposed rules. Some of these gaps relate to statutory constraints on your agencies' authority to regulate – such as the Act's failure to give consumers any right to prevent the disclosure of nonpublic personal information to affiliates of a financial holding company with whom they are doing business, or the joint agreement exemption from the "opt out" right with respect to disclosures to nonaffiliated third parties. Other gaps result from loopholes included in GLBA which provide for the specific exclusion of certain entities or certain practices from coverage under the Act.

We believe that Congress should work to pass legislation that builds on the proposed rule and addresses issues that the proposed rule does not cover. We welcome the President's pledge to press for the adoption of such legislation this year. We have sponsored financial privacy legislation (H.R. 3320/S. 1903) that we believe would accomplish the goal of providing the strong financial privacy protections that the American public deserves and expects. We hope to continue to work with your agencies and with other interested parties to promote the passage of meaningful financial privacy legislation. In the meantime, we urge you to issue final financial privacy regulations expeditiously, so that the public's financial information is protected as soon as possible.

The following are our comments on specific aspects of the proposed rules.

1. PURPOSE AND SCOPE

   We agree that the proposed rule's "Purpose and Scope" section is generally consistent with GLBA's requirements. The proposed rule identifies three broad purposes for the rule: 1) requiring financial institutions to provide notice to consumers about the institution's privacy policies and

practices; 2) describing the conditions under which a financial institution may disclose nonpublic personal information about the consumer to an unaffiliated third party; and 3) providing a method for consumers to "opt out" of the disclosure of such information to unaffiliated third parties, subject to certain exceptions.

We concur that the intent of the Congress in GLBA was for the rules to apply only to information about individuals who obtain a financial product or service from a financial institution to be used for personal, family, or household purposes. Congress limited the application in this manner because it was most concerned about the dangers and abuses which could occur if information about an individual or his and her family members were disclosed to others. Congress also believed that individuals were inherently less able to protect themselves against such disclosures than businesses. We would note, however, that businesses might also face certain risks if a financial institution with which they did business sold or disclosed nonpublic information about them. For example, such disclosures could reveal information of value to a competitor. While we believe that the most pressing priority is to protect the privacy of the individuals who are most vulnerable to privacy invasions, we also believe that your agencies should explore the nature and extent to which financial institutions may be disclosing nonpublic information about their business customers without their knowledge or consent.

We note that the federal banking agencies have sought comment on whether the GLBA privacy rules should apply to foreign financial institutions that solicit business in the United States but that do not have an office in the United States. We believe such institutions should be covered by the rules. Congress did not specifically exempt such foreign financial institutions from the privacy rules, and any U.S. consumers that do business with such institutions deserve the same level of privacy protections.

We also note that the NCUA Board has requested comment on whether federally insured corporate credit unions should be exempted from the rules. We believe that any natural person who is a consumer or a customer of such a credit union has the right to receive the same privacy protections as the consumers or customers of other types of financial institutions. We note that GLBA does not provide any specific exemption for such institutions. To the extent that such institutions may be functioning as a "credit union's credit union," we would suggest that, in general, the only exemptions that should be permitted to the rule would be those allowable under Section 502(e) of the Act, or which are otherwise deemed to be fully consistent with the purposes of the Act with respect to the protection of an individual's right to financial privacy.

We further note that the FTC has invited comment on the scope of the term "financial institution," which it notes is defined very broadly under GLBA. We agree that this term was defined quite broadly, and that Congress intentionally did this to assure that all of the institutions that fall within the definition should be covered by the Title V privacy rules. Congress intended not only for traditional financial activities to be covered by the Act, but also for nontraditional financial institutions or those engaged activities determined to be closely related to banking or usual in connection with the transaction of banking abroad. We do not believe that these activities should be interpreted narrowly by the Commission under the privacy regulations.

The financial services industry sought the expanded powers conferred by GLBA, and strongly supported the broad definition of financial institution created by the Act. With the expanded powers sought and obtained by the industry come some expanded responsibilities – including the responsibility to comply with the Act's privacy rules. As the FTC quite properly notes, "the plain meaning of the Act mandates this broad scope," which may include – but are not limited to – personal property appraisers, real estate appraisers, career counselors for employees in financial

occupations, digital signature services, courier services, real estate settlement services, manufacturers of computer software and hardware, travel agencies operated in connection with financial services, leasing real or personal property (or acting as agent, broker, or advisor in such leasing) where the lease is functionally equivalent to an extension of credit, acting as fiduciary, providing investment, financial, or economic advisory services, operating a travel agency in connection with financial services, check guaranty, collection agency, tax planning or preparation services, or providing financial data processing and transmission facilities or services, data bases, advice, or access to these by technological means. We also emphasize that, as the FTC has noted, many of the nontraditional financial institutions included within the broad scope of the Act do not have "consumers," establish "customer relationships," or provide financial products or services to individuals (as these terms are defined under GLBA). Consequently, such institutions will not be required to make the disclosures required by the Act.

2. RULE OF CONSTRUCTION

The various agencies have requested comment on whether including examples in the rules is useful in providing guidance as to how the rules should apply in specific situations. We believe that the use of such examples is useful, and that they generally help advance the goal of assuring that "plain language" is used in all proposed and final GLBA rules.

3. DEFINITIONS

We note that the definitions used in the proposed rule generally track the definitions set forth in the Act, and therefore limit our comments to a discussion of those definitions which we believe raise significant policy issues.

With respect to the definition of "clear and conspicuous," the agencies state that the proposed rule "does not mandate the use of any particular technique for making the notices clear and conspicuous, but instead allows each financial institution the flexibility to decide for itself how best to comply with this requirement." While we do not object to this approach, it raises the possibility that some financial institutions may attempt to evade the intent of the Act by crafting notices that are confusing to consumers, or fail to proper call attention to the information contained in the notice. Accordingly, we urge the agencies to exercise vigorous oversight over how the institutions within their respective jurisdictions are complying with this requirement. Such oversight should include surveys, examinations or audits focused on the nature and adequacy of industry notices, and appropriate enforcement action against institutions that violate the requirements by providing confusing disclosures full of legal gobbledygook.

With respect to the definition of "customer relationship," we have concerns that the proposed definition may fail to give consumers appropriate privacy protections under certain circumstances. We agree that the term covers both situations in which there is a continuing relationship as well as circumstances in which there is a one-time transaction. We have concerns, however, with the agencies' proposed exemptions for certain types of "one time transactions."

The specific examples cited by the agencies of situations in which a customer relationship would not be considered to have been established for the purposes of the rule are: 1) using (either once or on repeated occasions) an automated teller machine at a bank or credit union at which a consumer transacts no other business; 2) cashing a check at such an institution; 3) purchasing travelers checks or money orders, or making a wire transfer at such an institution; 4) purchasing airline tickets; 5) purchasing securities from a broker who has provided the service as an accommodation

but does not open an account for the individual; and 6) liquidating securities for a consumer when the broker does so on a one-time basis.

While we understand that, as a practical matter, it may not be feasible for a financial institution to provide such consumers with the annual notices required under the Act, we nevertheless believe that these individuals deserve the right to say "no" to having information about their transactions or experiences with the institution disclosed to others. We are concerned that the proposed rules could be read to allow a financial institution to fail to provide such individuals with the required notices if the institution intends to disclose nonpublic personal information about these consumers to nonaffiliated third parties outside the exceptions. We do not believe that was the intent of the Act. We therefore urge you to clarify that while a financial institution may not be required to provide annual notices to consumers who have engaged in "one time transactions" with the institution, such consumers would still be afforded prior notice and a right to opt-out before the institution makes disclosures about them to any non-affiliated third party. Such consumers should also receive the protections against reuse of information afforded under the Act.

With respect to the definition of "financial institution," in addition to the comments we have outlined in Section 1 of our comments, we would like to comment on some of the exceptions to the definition.

First, we note that the FTC proposed rule invites comment on its interpretation regarding the Act's exception for institutions chartered by Congress to engage in secondary market sales and similar transactions related to customers. This particular exception applies only as long as the institution does not sell or transfer nonpublic personal information to a third party. The FTC has interpreted this exception to its proposed Rule to apply even if the chartered institution sells or transfers information as permitted by the exceptions to the notice and "opt out" requirements set forth in Sections 313.10 and 313.11 of the proposed rules. We concur with this interpretation, and believe that those entities that receive consumers' nonpublic personal information from such institutions are nonetheless subject to the Rule's limitations on reuse. We also agree that such chartered financial institutions should be required to enter into a confidentiality agreement with those nonaffiliated third parties with which they share information. In addition, we believe that the term "transfer" (which one of us added to this provision of the Act by an amendment offered during the Conference Committee) should be interpreted very broadly. Such term should cover both an instance in which such an institution has physically transferred data about a consumer to a nonaffiliated third party (either for or without monetary or other compensation), as well as any instances in which the information is transferred from a the institution's secondary market/securitization activities to any other business line engaged in providing a product or service to a nonaffiliated third party that involves the use of such information.

Second, we strongly object to the exemptions contained in Section 509(3)(B) and (C) of the Act. These exemptions were not added due to any reasoned analysis or determination that persons subject to the jurisdiction of the Commodities Futures Trading Commission under the Commodity Exchange Act, the Federal Agricultural Mortgage Corporation, or any entity chartered and operating under the Farm Credit Act of 1971 should not be required to give their consumers and customers the same level of privacy protections required for other types of financial institutions. Indeed, commodity pool operators, futures commission merchants, Farmer Mac, and other agricultural lending institutions should be required to provide comparable privacy protections for their consumers and customers, including notice and the right to say "no" to having nonpublic personal information disclosed to others. The only reason these entities were excluded from the coverage of the Act was that certain Members of the House Agriculture Committee objected to their inclusion, based on jurisdictional concerns. We regret that the political decision to

accommodate such concerns has left certain consumers without any assurance that they will receive any privacy protections whatsoever. We therefore urge your agencies to endorse legislative reforms that would rectify this situation.

With respect to the definition of "nonpublic personal information," we concur with your determination that this term includes (but is not limited to) any list, description, or other grouping of consumers – and publicly available information that is derived using any nonpublic personal information other than publicly available information. We note that the agencies have set forth two alternatives concerning the treatment, for purposes of defining "nonpublic personal information," or information that can be obtained from sources available to the general public. We strongly urge the agencies to adopt "Alternative A." As we understand Alternative A, information is only "publicly available information" if the financial institution actually obtains the information from a public source, such as government records, widely distributed media, or government-mandated disclosures. Under Alternative B, information could be deemed "publicly available information" if it theoretically could be obtained from a public source, even if the institution had not done so and instead relied on information provided by the consumer or by other parties. We believe that Alternative A should be adopted because, unless the financial institution has actually obtained the data from a public source it cannot be certain that the information is, in fact, publicly available. We fear that if Alternative B were adopted, financial institutions may treat information that they have received from the consumer as publicly available even if the information can not actually be obtained from a public source. Only by requiring the institution to actually obtain the data from a public source can there be adequate assurance that customer-provided information is fully protected from disclosure.

With respect to the definition of "personally identifiable financial information," we generally concur with the treatment of this term in the proposed rule. We would like to emphasize, however, that we agree with the agencies that the term includes certain types of health information. We therefore suggest that the examples used in the proposed rule should include a specific reference to health information, and that the notices provided to consumers include a specific reference to the institution's policies and practices with respect to the disclosure of health information. In defining health information for the purposes of the rule, we suggest that you use a definition comparable to that contained in the recently proposed Department of Health and Human Services (HHS) regulations that implement the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

We note that the HIPAA rules provide some additional limitations on the circumstances under which certain types of medical information may be disclosed by certain types of institutions. However, we also note that the proposed HHS rule excludes the vast majority of health information and certain insurance entities. These include automobile insurers, property and casualty insurers, as well as disability insurers. It is also possible that other types of financial institutions, such as a bank, might obtain access to medical information. Neither the proposed HHS regulations nor your agencies' proposed regulations provides sufficient protection against a financial institution disclosing sensitive details regarding a consumer's medical history to affiliates, or to third parties with whom they have a joint agreement pursuant to the exception provided in Section 502(b)(2) of the Act. We believe it essential that the loopholes in the current law that create these gaps in coverage of medical privacy protections be eliminated, and we urge your agencies to support legislation to achieve this goal.

Finally, we note that the agencies have requested comment on whether information obtainable from a site available to the general public on the Internet without requiring a password or similar restriction should be considered to be publicly available. While much of the information made

available in this fashion should properly be considered to be publicly available, there may be some circumstances in which such information should not be appropriately considered publicly available. For example, if a computer hacker should obtain access to nonpublic personal information and then post it on an Internet Web site, such information should not be considered to be publicly available.

4. INITIAL NOTICE OF PRIVACY POLICIES AND PRACTICES

The proposed rules require financial institutions to: 1) provide an initial notice of their privacy policies and practices; and, 2) to provide individuals with a notice prior to the time that the institution establishes a customer relationship with the individual. These notice requirements are an essential foundation for providing consumers with financial privacy protection. Consumers have a right to obtain knowledge regarding what information is being collected about them and to receive notice of the privacy practices and policies of the entities with which they are transacting business. We agree that such notices must be clear and conspicuous, and that they must be designed to call attention to the nature and significance of the information they provide. They must also accurately reflect the institution's privacy policies and practices. Consumers also should be informed of any changes in such privacy policies and practices before they occur, so consumers can take appropriate action to assure that their rights are protected.

We agree that the notice may be delivered in writing, or if the consumer agrees, electronically. We also agree that oral notices alone would not be sufficient to comply with the Act. We must note the irony that the proposed rules establish a consumer "opt in" requirement for electronic delivery of a privacy notice, but fail to provide consumers with an across-the-board "opt in" right to block disclosure of nonpublic personal information to affiliates or unaffiliated parties. We will discuss the "opt in" versus "opt out" issue further below.

We have some concerns about the vagueness of the proposed exemptions to allow subsequent delivery of notice. The proposed rules state the initial notice may be provided "within a reasonable time after" the financial institution establishes the customer relationship. What is a reasonable time? Is it one week, two weeks, a month, or six months? Under the proposed rule, an institution could establish a customer relationship orally and the customer could agree to receive the notice thereafter. Unless there is greater assurance that the customer will receive the notice promptly, we cannot be confident that the customer will have the information that he or she needs to assess the privacy policies and practices of the financial institution and determine whether to exercise their opt-out rights. We therefore believe that the rule should require that the initial notice should be provided in writing no later than the time the customer relationship is established. This will allow the consumer/customer to review and evaluate the institution's privacy policies and practices at the inception of the relationship, and facilitate the ability of the consumer to compare the policies and practices offered by rival or competing institutions. Promoting market incentives to provide consumers with greater privacy protections was one of the purposes of the disclosure provisions of the Act.

5. ANNUAL NOTICE OF PRIVACY POLICIES AND PRACTICES

We generally support the provisions of the rule regarding the provision of annual notice to customers. An annual notices is useful in reminding customers of: 1) their financial institution's policies and practices; 2) the nature and scope of the nonpublic personal information that the institution is collecting about them; 3) what information is disclosed to affiliates or nonaffiliated third parties; and, 4) the consumer's rights to limit the disclosure of such information to other parties by "opting out."

6. INFORMATION TO BE INCLUDED IN INITIAL AND ANNUAL NOTICES

We generally support the proposed rules' requirements with respect to what information shall be included in the initial and annual notices, with the exception of the specific concerns and comments we outline below.

We note that the proposed rule closely tracks the specific language contained in Sections 503(a) and 503(b) of the Act. Section 503(a) sets out the general requirement for a financial institution to provide consumers with clear and conspicuous disclosures that describe the institution's policies and practices with respect to disclosing nonpublic personal information to affiliates and nonaffiliated third parties, disclosing information about persons who have ceased to be customers of the institution, and protecting the nonpublic personal information of consumers. Section 503(b) mandates that such disclosures include certain specific elements that Congress has determined must be included in such disclosures.

We agree with the agencies' assessment that the Act requires a financial institution's notice to address disclosures of nonpublic personal information to both affiliates and nonaffiliated parties, and that such disclosures should be reasonably designed to be meaningful to consumers. However, we also believe that financial institutions should have to inform consumers if they are disclosing information pursuant to one of the exceptions. We do not believe that merely stating that a financial institution makes disclosures as permitted by law to nonaffiliated third parties in addition to those described in the notice is adequate to inform consumers regarding the nature and extent to which the consumers information is being transferred to other business entities.

We are also concerned that the proposed rule fails to provide consumers with any notice regarding whether the financial institution provides the consumer with the right to obtain access to and correct nonpublic personal information the institution has collected about them and is disclosing to affiliates or nonaffiliated third parties. We believe that providing consumers with access and correction rights is a critical part of any fair information practice. We note that the Fair Credit Reporting Act (FCRA) provides consumers with access and correction rights with respect to credit reports. However, it is our understanding that transactional or experiential information a financial institution collects about its consumers is generally exempt from the requirements of the FCRA, including the right of access and correction. This FCRA exemption covers much of the information collected by the financial institutions regulated under GLBA. For this reason, it is essential that the access and correction issue be addressed in the proposed rule. We also note that the proposed HHS medical privacy regulations under HIPAA also provide consumers with access and correction rights, and that the Department of Commerce, in negotiating a "safe harbor" for U.S. firms' treatment of nonpublic personal information of citizens of the European Union, has included access and correction rights for EU citizens. We do not believe that U.S. citizens should receive a lower level of privacy protection from financial institutions than such institutions provide to EU citizens, or than health plans otherwise provide to U.S. citizens under the HIPAA medical privacy rules.

We believe that the authorities provided in Section 503, in combination with the powers granted to your agencies in Section 501 to require financial institutions to comply with standards that safeguard the security, confidentiality and integrity of customer records, can and should be read to confer to your agencies the power to require financial institutions to afford their customers access and correction rights and with notice regarding such rights. We therefore urge you to revise your rule to provide such rights to U.S. customers of financial institutions. We do not believe that this would impose an impossible burden on U.S. firms, as many of these firms operate in the EU market and already have to provide access and correction rights to their European customers in

order to qualify for the safe harbor. Moreover, to the extent that such institutions or their affiliates should fall within the purview of the HIPAA privacy regulations or the FCRA, they already have to provide certain access and correction rights.

At a more fundamental level, however, we believe that individuals should have a right to obtain access to the information that is being collected about them by a financial institution with whom they do business and that is disclosed to affiliates or to nonaffiliated parties. Consumers should also have the right to have any inaccurate or misleading information corrected. This right is an essential protection for consumers. It assures that a financial institution's decision regarding whether to approve a loan, issue an insurance policy, or otherwise provide a financial product or service to a consumer is not influenced by inaccurate derogatory information about the customer. Providing consumers with such a right also serves as an important check on a financial institution's amassing and disclosing disturbingly detailed profiles about consumers, as such institutions would not want their customers to see that the institution was preparing such profiles, and would be more likely to limit their data collection and disclosures accordingly.

While we feel very strongly that you should provide consumers with full access and correction rights, if you should decide not to do so, we would argue – in the alternative – that your agencies should, at the very minimum, require all financial institutions to include a specific disclosure to consumers indicating whether the institution's privacy policies and practices include giving customers access and correction rights. In the event such rights are not provided, the institution should be required to explain why the institution has declined to provide the consumer with the ability to obtain access to the information the institution is disclosing to its affiliates or to third parties, and why the institution has chosen not to give its customers correction rights. While such a notice would not achieve the objective of assuring that such rights will in fact be provided, it would at least have the effect of raising consumer awareness that their financial institutions were refusing to provide them with such rights – a development which might ultimately give institutions an incentive to provide their customers with such rights.

7. LIMITATION ON DISCLOSURE OF NONPUBLIC PERSONAL INFORMATION ABOUT CONSUMERS TO THIRD PARTIES

We believe that the limited third party "opt out" right provided under the proposed rule fails to provide consumers with meaningful privacy protections. We note that this failure is largely the result of Congress' failure to provide consumers with a right to say "no" to disclosures to both affiliates and to nonaffiliated third parties, Congress' decision to adopt a low "opt out" threshold rather than a higher "opt in" threshold, and the giant loophole created by the exception in Section 502(b)(2) of the Act.

First, with respect to affiliate sharing, we do not believe that a consumer's privacy rights should be sacrificed on the altar of the purported "synergies" resulting from the expanded affiliations available under GLBA. In general, we believe that financial institutions should have to obtain the consent of the consumer before they disclose nonpublic information about the consumer to any other entity or for any purpose other than the original purpose for which the information was provided. We believe it is wrong to allow financial services holding companies to freely transfer information between banking affiliates, securities affiliates, insurance affiliates, and any other affiliates without first obtaining such consent. Before such information is transferred to an affiliate of an institution with whom a consumer transacts business, the consumer should "opt in" to the disclosure.

Second, with respect to the standard of consent, we strongly support an "opt in" standard, in which

the financial institution must obtain the permission of the consumer before disclosing nonpublic personal information about the consumer to others. "Opt in" puts the burden on the financial institution to convince the consumer to avail themselves of the "synergies" available in the form of new and innovative financial products or services that may be of potential interest to them. Under such a regime, if the consumer objects or declines to respond, the institution cannot disclose the information. An "opt out" regime, in contrast, puts the burden on the consumer to affirmatively object in order to protect the privacy of their nonpublic financial information. If a consumer fails to respond to or does not understand the notice provided under the rule, the institution is free to disclose the consumers' information.

We would note that in many other areas of the law, "opt in" is the norm. For example, a consumer "opt in" is required before a tax preparer could transfer information from a consumer's tax return to a financial advisory affiliate to provide the consumer with financial planning advice. An "opt in" is required before a video rental store can provide information regarding a consumer's videocassette rentals to others. "Opt in" is required before telephone companies can transfer information about what telephone numbers a consumer calls or the whereabouts of the cellular phone the consumer is using to other parties. "Opt in" is required before cable television companies can provide information about what pay per view movies a consumer is watching to other parties. We see absolutely no reason why a consumer's most sensitive financial information should be accorded a lower level of protection than the law affords in these other areas. We therefore urge your agencies to support the enactment of legislation, such as H.R. 3320 and S. 1903, which would provide consumers with an across-the-board "opt in" right for both affiliate and third party information disclosures.

With respect to the specifics of the proposed "opt out" requirements of the proposed rule, we would offer the following comments.

First, with respect to joint accounts, we believe that if any party to a joint account elects to exercise their "opt out" right, then the opt out should become effective. We do not believe it is feasible to protect the privacy of one party who has elected to "opt out," while allowing information to be disclosed about another party to the account that has not exercised his or her right to "opt out."

Second, in the event that an individual does not exercise his or her "opt out" right when first presented with the opportunity, but then subsequently elects to do so, we believe that the rule should proscribe a specific timeframe within which the institution must cease disclosing information about the consumer to nonaffiliated third parties. Currently, the proposed rule provides no specific guidance as to how long this period could be. The federal banking agencies state that they have "considered whether to include a time limit by which financial institutions must effectuate a consumer's opt out election, but decided that the wide variety of practices of financial institutions made one limit inappropriate." We disagree. Despite the variations in business practices in the industry, we believe that it should be possible to establish an outer deadline by which a financial institution must comply with the consumer's "opt out" decision. We would suggest that an institution should comply with the consumers request within 30 days – the same amount of time that the rule provides for the consumers to exercise their "opt out" rights in the first instance. Given the rapid pace of technological change occurring in the financial services industry, and the industry's long record of taking the lead in applying telecommunications and computer technologies to meeting the needs of its consumers, we have every confidence that the industry will be able to comply with such a deadline.

8. FORM AND METHOD OF PROVIDING OPT OUT NOTICE TO CONSUMER

Given the inherent limitations in the authorities provided to the agencies under the Act that preclude you from adopting an across-the-board "opt in" for both affiliates and nonaffiliated third parties, the proposed rule contains many welcome features to ensure that the consumer is informed regarding their right to "opt out" and is provided with a mechanism for exercising that right.

We believe that it is essential for the rule to make it as easy as possible for those consumers who wish to "opt out" to do so. Accordingly, we agree that it should not be acceptable for institutions to require a consumer to write their own letters to the institution in order to exercise their "opt out" rights. We also strongly support requiring financial institutions to accept "opt outs" through any measures the institution has already established to communicate with consumers. Therefore, in response to the specific requests for comments in the FTC and SEC proposed rules, we agree that the rule should require that if an institution establishes a toll-free telephone number or Web site through which it communicates, transacts business, or otherwise interacts with the consumer, that such telephone number or Web site should also be required to accept "opt outs." We also believe that if the institution provides the notices and disclosures required under the rule in electronic form, the institution should also be required to accept "opt outs" in such form. Without such requirements, some financial institutions may seek to reduce the number of consumers who elect to exercise their "opt out" option by making it technically more difficult, time-consuming, or troublesome to do so.

We note that the proposed rule also provides for procedures through which a financial institution must notify its customers regarding changes in the institution's privacy policies and practices and give the customer a new opportunity to "opt out." We have a few comments regarding this part of the rule.

First, the rule should make it clear that those customers who have already "opted out" do not have to do so again each time the institution revises its privacy policies or practices. Unless such customers affirmatively elect to reverse their previous "opt out" decision, their information should continue to be protected from disclosure.

Second, we believe that additional guidance is needed to define what constitutes "a reasonable period of time" before a financial institution is permitted to disclose information according to the terms of the revised notice. The consumer should be afforded the same 30 days to exercise their opt-out right following the receipt of a notice from the institution that it has revised its privacy policies and practices that the rule allows following the initial notice. Here again, the financial institution should be required to comply with the consumer's request within 30 days of its receipt.

9. EXCEPTION TO OPT OUT REQUIREMENTS FOR SERVICE PROVIDERS AND JOINT MARKETING

We are unalterably opposed to the exception contained in Section 502(b)(2) of GLBA for service providers and joint marketing, and regard this loophole as one of the principle shortcomings of the Act. This exception makes a mockery of the "opt out" right conferred in Section 502(b) of the Act. It invites financial services firms to entirely circumvent the restrictions imposed by this subsection by merely entering into a formal written contract with another financial institution in which the parties jointly offer, endorse, or sponsor a financial product or service, and agree to maintain the confidentiality of the information disclosed. Given the breadth of the definition of "financial institution" under the Act and the vast array of new powers conferred to them under the bill, this exception could allow financial institutions to disclose sensitive nonpublic information that could be used for telemarketing purposes – potentially inviting a repetition of some of the same abuses

that were seen in the State of Minnesota's recent litigation against US Bancorp and the State of New York's case against Chase. We therefore urge your agencies to support legislation that would repeal this loophole in the law.

Within the limitations of the scope of authority provided under the exception, we strongly urge the rule to require that, if a financial institution wishes to use the exception contained in Section 502 (b)(2), it should be required to disclose not only that it will provide nonpublic personal information about the consumer to such third parties, but also that it has declined to give the consumer any right to "opt out" of having this information be so disclosed. Moreover, we suggest that the rule require the institution to explain the reasons why the institution has declined to provide its customers with such a right.

10. EXCEPTIONS FOR PROCESSING AND SERVICING TRANSACTIONS

We note that this section of the rule largely restates the specific statutory exceptions created under GLBA for processing and servicing transactions.

We would suggest, however, that the agencies consider directing financial institutions to make every effort to avoid transferring personally-identifiable nonpublic information about consumers pursuant to these exceptions where it is feasible to instead provide such information in "de-identified form." For example, it may be possible to provide de-identified information to the entities described in Section 502(e)(4), or to a prospective purchaser pursuant to the exception set forth in Section 502(e)(7) of the Act.

In addition, we are concerned that for both these and other exceptions to the notice and "opt out" requirements, the proposed rule imposes no limitations on the amount or type of information disclosed. While the disclosure of some nonpublic information in these circumstances may be legitimate, the rule should impose some limitations, so that the disclosures that are made pursuant to the exceptions are the minimum necessary to accomplish the purpose of the disclosure under the exception.

11. OTHER EXCEPTIONS TO OPT OUT REQUIREMENTS

With respect to the exception allowed for disclosures made with the consent or at the direction of the consumer, we strongly urge the agencies not to permit this exemption to become a mechanism for evading the notice and "opt out" requirements otherwise established by the Act. Accordingly, we agree that a "consent" that is not clearly made by the consumer, such as a line buried in a document or a negative option not clearly explained to the consumer should not be permitted. Generally, we also urge the agencies to establish additional safeguards to minimize the potential for confusion or abuse. For example, we believe that such consent should be required to be in written form, or in a distinct Web page, and that it be effective for only a limited period of time and only for a distinct purpose. For example, no general authorization for disclosures to broad classes or categories of nonaffiliated third parties should be permitted, as opposed to the type of specific authorization for a specific disclosure mentioned in the example.

12. LIMITS ON REDISCLOSURE AND REUSE OF INFORMATION

We agree that the agencies' rules should require a financial institution that discloses nonpublic personal information to a nonaffiliated third party to develop policies and procedures to ensure that the third party complies with the limits on redisclosure of that information. As the federal

banking agencies noted in their request for comment, the types of joint marketing arrangements envisioned under the Act can have adverse reputational effects if the nonaffiliated third parties that receive information pursuant to such agreement fail to protect its confidentiality. Mandating that financial institutions establish procedures to ensure that the third parties that have received nonpublic personal information from the institution also have established strong internal controls to safeguard the confidentiality, integrity, and security of such data is an important step in reducing the potential for misuse of the information. Such procedures also should provide mechanisms for ensuring that those consumers who subsequently decide to exercise their "opt out" rights will have their information promptly deleted from the unaffiliated third party's databases.

With respect to the meaning of the word "lawful" as that term is used in section 502(c), we do not believe that third parties that have received information from a financial institution may then proceed to retransfer the information to others pursuant to the joint marketing exception set forth in Section 502(b)(2) of the Act. In such cases, the originating financial institution may not even be a party to the subsequent disclosure. To allow nonaffiliated third parties that receive information from a financial institution to transfer this information to other nonaffiliated third parties, who in turn can transfer the information to yet other nonaffiliated third parties, would subvert one of the key purposes of the Act. What assurance could the consumer have that such disclosures were consistent with the privacy policies and practices that had been disclosed to them by the originating financial institution at the time that the consumer elected not to exercise their right to "opt out?" For those consumers who did exercise their "opt out" rights, but had their information transferred to nonaffiliated third parties due to the joint marketing exception, the situation is even worse. Here, the consumer wanted privacy, was denied the right to say "no," and now might face a cascading series of information transfers over which he or she has no control. While we oppose the joint marketing exception, we do not believe it was the intent of this provision to allow such a situation. Instead, proponents of this provision argued during the Congressional debate that it would be used to allow small financial institutions that could not take advantage of the affiliate structure permitted under the Act to nevertheless offer their customers different types of financial products and services. It was never argued that the nonaffiliated third parties who receive information pursuant to this exemption should then be free to transfer it to any other nonaffiliated third party with whom they have a joint marketing agreement.

13. LIMITS ON SHARING OF ACCOUNT NUMBER INFORMATION FOR MARKETING PURPOSES

We note that the proposed rule closely tracks the statutory language of the Act. As the agencies have noted, there are no exceptions to the flat prohibition established by Section 502(d) of the Act. Language in the Statement of Managers contained in the Conference Report on S. 900 – the bill that ultimately became GLBA – urges the agencies to adopt an exception to this section that would permit disclosures of account numbers in certain instances where the disclosure is in an encrypted, scrambled or similarly coded form, is expressly authorized by the customer, and is necessary to service or process a transaction expressly requested or authorized by the customer.

Some of us served as conferees on this bill, and know from direct personal experience with the legislative history of the bill and the actions of the Conference Committee that this language was added to the report by the Committee staff without debate or discussion during any meeting of the Conference Committee. Indeed, we are aware that attempts were made to convince Members of the Conference Committee to offer an amendment to this section of the Act -- all without success. We therefore urge the agencies to view this Manager's language with healthy skepticism.

We would note that the language in the Statement of the Managers is directly at odds with the plain meaning of the prohibition set forth in Section 502(d), which was intended to respond to a number of widely publicized abuses involving the provision of bank customers' credit card information to telemarketing firms. In light of these past abuses and the threat that they might be repeated, we strongly support the agencies' decision not to include the type of exception envisioned in the Statement of the Managers. It is a long established principle that legislative history – including Managers' language -- cannot override clear legislative language to the contrary. We also believe that the risks associated with allowing nonaffiliated third parties with direct access to a consumer's account are very great. We would therefore prefer that you adopt this part of the proposed rule unchanged.

In the event that you decide to grant any exceptions to the flat prohibition in the Section (which we question whether you have the authority to do), we would argue – in the alternative -- that the only circumstance in which the agencies should consider allowing any disclosure of a consumer's account numbers would be if the consumer provided his or her explicit prior consent (i.e., has "opted in") to such a disclosure. In such circumstances, the rule should provide for special notice requirements that would help the consumer understand the potential adverse consequences of allowing disclosure of his or her account numbers to third parties, a mandate that such disclosure may only be made in encrypted form, and that any marketing firm receiving such encrypted information may not be provided with the key to decipher the encoded number.

14. PROTECTION OF THE FAIR CREDIT REPORTING ACT

We note that this section merely restates the statutory provisions of Section 506 of the Act.

15. RELATION TO STATE LAWS

We agree that the privacy provisions of GLBA do not preempt any state law that provides greater protections than those provided by this Act. Those of us who served as Conferees on S. 900 strongly supported the adoption of this provision in the Conference. Our intent in doing so was to assure that states were free to adopt stronger privacy protections, including, but not limited to laws giving consumers the ability to "opt in" to both affiliate and nonaffiliated third party disclosures of nonpublic personal information, stronger state laws regarding medical privacy, or any other additional protections which the states deemed necessary in addition to the "floor" of protections provided under federal law.

16. EFFECTIVE DATE; TRANSITION RULE

We believe that six months following adoption of a final rule should be sufficient time to enable financial institutions to comply with the rule's requirements. We also believe that individuals who are already customers of a financial institution as of the effective date of the rule should be provided with the initial notice within 30 days of the effective date of the rule.

17. CONCLUSION

Protecting the consumer's fundamental right to financial privacy is essential to assuring that the public will have confidence that the changes brought about by GLBA are consistent with the public interest. While we commend you for your efforts to craft privacy protections in this area, we believe that flaws in the underlying statute you are seeking to interpret and enforce place severe limitations on your agencies' ability to protect the American public from invasions into their privacy. We believe that in order to

address these flaws in the legislative framework under which you are operating, Congress must adopt new legislation, along the lines of H.R. 3320 and S. 1903. We urge you to endorse such legislative reforms. In the interim, we ask you to adopt the proposed changes we have outlined above. We look forward to reviewing the comments of others on the proposed rule and your response to our comments.

Sincerely,

/s /s

Edward J. Markey
Co-Chair
Congressional Privacy Caucus

Richard C. Shelby
Co-Chair
Congressional Privacy Caucus

/s /s

Richard H. Bryan
Co-Chair
Congressional Privacy Caucus

Joe Barton
Co-Chair
Congressional Privacy Caucus

s/ s/

Bill Luther
Member
Congressional Privacy Caucus

Jay Inslee
Member
Congressional Privacy Caucus

s/ s/

Jan Schakowsky
Member
Congressional Privacy Caucus

Fortney "Pete" Stark
Member
Congressional Privacy Caucus

s/ s/

Maurice D. Hinchey
Member
Congressional Privacy Caucus

Henry Waxman
Member
Congressional Privacy Caucus